RECEIVED
CENTRAL FAX CENTER
JUN 18 2009

AMENDMENT TO THE CLAIMS

1. (Currently amended) A method for developing a program which is to be installed in a system having an LSI device, the LSI device having a secure memory which includes an unrewritable area, the method comprising the steps of:

providing another LSI device having the same structure as that of the LSI device;

setting the provided LSI device to a development mode based on an inherent and permanent key information for the development mode, which is implemented in the unrewritable area of the LSI device in advance, so that the provided LSI device is used as a development LSI device, the development mode being different from a product operation mode employed at the times of program installation and product operation, the inherent and permanent key information for the development mode being different from an inherent and permanent key information for the product mode; and

developing the program on the development LSI device.

2. (Previously presented) The method of claim 1, wherein the operation of the provided LSI device is restricted such that when being set to the development mode, the provided LSI device can execute a raw (binary) program, and when being set to the product operation mode, the provided LSI device cannot execute a raw (binary) program with an executable form but can execute an encrypted program.

3. (Original) The method of claim 1, further comprising the step of encrypting the program developed on the development LSI device at the program development step.

4. (Original) The method of claim 1, wherein the operation of the LSI device is restricted such that when being set to the development mode, the LSI device cannot generate a key for encrypting a raw (binary) program.

5. (Original) The method of claim 1, further comprising the steps of:

providing an LSI device having the same structure as that of the LSI device;

setting the provided LSI device to a key-generation mode so that the provided LSI device is used as an key-generation LSI device, the key-generation mode being different from the development mode and the product operation mode; and

installing an encrypted key-generation program in the key-generation LSI device and executing the key-generation program to generate a key.

6. (Original) The method of claim 5, wherein the operation of the LSI device is restricted such that when being set to the key-generation mode, the LSI device cannot execute a raw (binary) program.

7. (Original) The method of claim 5, further comprising the steps of:

providing an LSI device having the same structure as that of the LSI device;

setting the provided LSI device to an administrator mode so that the provided LSI device is used as an administrator LSI device, the administrator mode being different from the development mode, the product operation mode, and the key-generation mode; and

developing the key-generation program and encrypting the developed key-generation program with any key on the administrator LSI device.

Application No.: 10/624,481

8. (Currently amended) A program development supporting system for supporting development of an encrypted program [[,]] which is to be installed in a system having an LSI device, the LSI device having a secure memory which includes an unrewritable area, the system comprising:

a development LSI device having the same structure as that of [[an]] the LSI device on which the encrypted program runs; and

an external memory for storing a raw (binary) program, wherein

the development LSI device includes a secure memory for storing encrypted common key information regarding a raw common key different from an inherent and permanent key used for product mode, which is implemented in the LSI device in advance, and

the development LSI device is capable of executing

a first step of obtaining the raw common key from the common key information stored in the secure memory, and

a second step of encrypting the raw (binary) program input from the external memory using the raw common key.

9. (Previously presented) A program development supporting system for supporting development of an encrypted program, comprising:

a development LSI device having the same structure as that of an LSI device on which the encrypted program runs; and

an external memory for storing a raw (binary) program, wherein

the development LSI device includes a secure memory for storing common key information regarding a raw common key, and

the development LSI device is capable of executing

a first step of obtaining the raw common key from the common key information stored in the secure memory, and

a second step of encrypting the raw (binary) program input from the external memory using the raw common key,

wherein:

the common key information includes an encrypted common key which is obtained by encrypting the raw common key with a raw first intermediate key and an encrypted first intermediate key which is obtained by encrypting the raw first intermediate key with a second intermediate key; and

the first step includes the step of obtaining the raw common key using the encrypted common key, the encrypted first intermediate key and a program encryption seed.

10. (Currently amended) A program development supporting system for supporting development of an encrypted program [[,]] which is to be installed in a system having an LSI device, the LSI device having a secure memory which includes an unrewritable area, the system comprising:

a development LSI device having the same structure as that of an LSI device on which the encrypted program runs; and

an external memory for storing a raw (binary) program, wherein

the development LSI device includes

a secure memory for storing encrypted common key information regarding a raw common key different from an inherent and permanent key used for product mode, which is implemented in the LSI device in advance, and

a boot ROM for storing a boot program, and

by executing the boot program stored in the boot ROM, the development LSI device executes

a first step of obtaining a raw common key from the common key information stored in the secure memory, and

a second step of encrypting the raw (binary) program input from the external memory using the raw common key.

11. (Previously presented) A program development supporting system for supporting development of an encrypted program, comprising:

a development LSI device having the same structure as that of an LSI device on which the encrypted program runs; and

an external memory for storing a raw (binary) program, wherein

the development LSI device includes

a secure memory for storing common key information regarding a raw common key, and

a boot ROM for storing a boot program, and

by executing the boot program stored in the boot ROM, the development LSI device executes

a first step of obtaining a raw common key from the common key information stored in the secure memory, and

a second step of encrypting the raw (binary) program input from the external memory using the raw common key,

wherein:

the common key information includes an encrypted common key which is obtained by encrypting the raw common key with a raw first intermediate key and an encrypted first intermediate key which is obtained by encrypting the raw first intermediate key with a second intermediate key; and

the first step includes the step of obtaining the raw common key using the encrypted common key, the encrypted first intermediate key and a program encryption seed.

12. (Withdrawn-Previously presented) A method for installing an encrypted program in a key-implemented system which includes an external memory and an LSI device having a secure memory, the method comprising:

an initial value setting procedure for storing common key information regarding a raw common key and inherent key information regarding a raw inherent key in the secure memory;

a first step of obtaining in the LSI device the raw common key from the common key information stored in the secure memory;

a second step of decrypting in the LSI device a common key-encrypted program supplied from the external memory into a raw (binary) program using the raw common key obtained at the first step;

a third step of obtaining in the LSI device the raw inherent key from the inherent key

information stored in the secure memory;

a fourth step of encrypting in the LSI device the raw (binary) program obtained at the second step using the raw inherent key obtained at the third step, thereby obtaining an inherent key-encrypted program; and

a step of installing the inherent key-encrypted program obtained at the fourth step in the external memory.

13. (Withdrawn) The method of claim 12, wherein

the LSI device includes a boot ROM for storing a boot program, and

the LSI device executes the boot program stored in the boot ROM, thereby executing the first to fourth steps.

14. (Withdrawn) The method of claim 12, wherein

the inherent key information is stored in an unrewritable area of the secure memory.

15. (Withdrawn) The method of claim 12, wherein

the common key information includes an encrypted common key which is obtained by encrypting the raw common key with a raw first intermediate key and an encrypted first intermediate key which is obtained by encrypting the raw first intermediate key with a second intermediate key; and

the first step includes the step of obtaining the raw common key using the encrypted common key, the encrypted first intermediate key and a program encryption seed.

16. (Withdrawn) The method of claim 12, wherein:

the inherent key information includes an encrypted inherent key which is obtained by encrypting the raw inherent key with a raw first intermediate key and an encrypted first intermediate key which is obtained by encrypting the raw first intermediate key with a second intermediate key; and

the third step includes the step of obtaining the raw inherent key using the encrypted inherent key, the encrypted first intermediate key and a program encryption seed.

17. (Withdrawn) The method of claim 12, wherein the inherent key information is an inherent ID which is inherent to the LSI device.

18. (Previously presented) The method of claim 1, wherein the inherent and permanent key information is not outputted from the LSI device in both the development mode and the product operation mode.